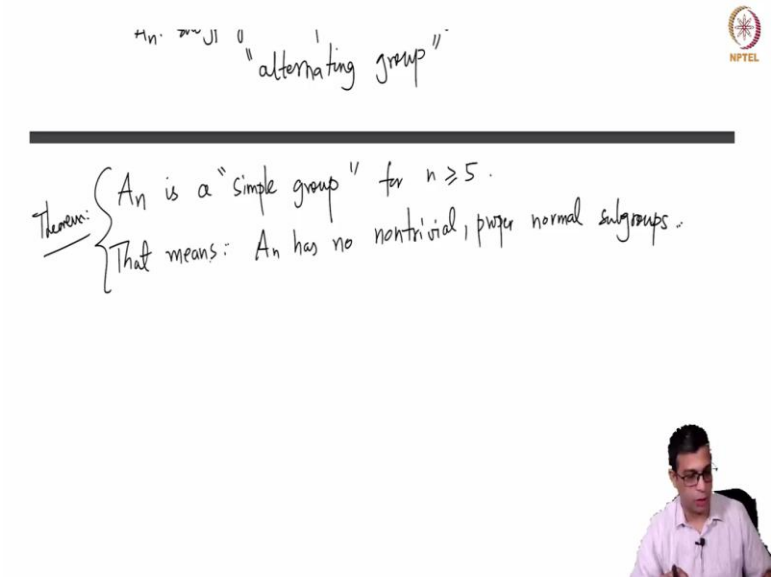
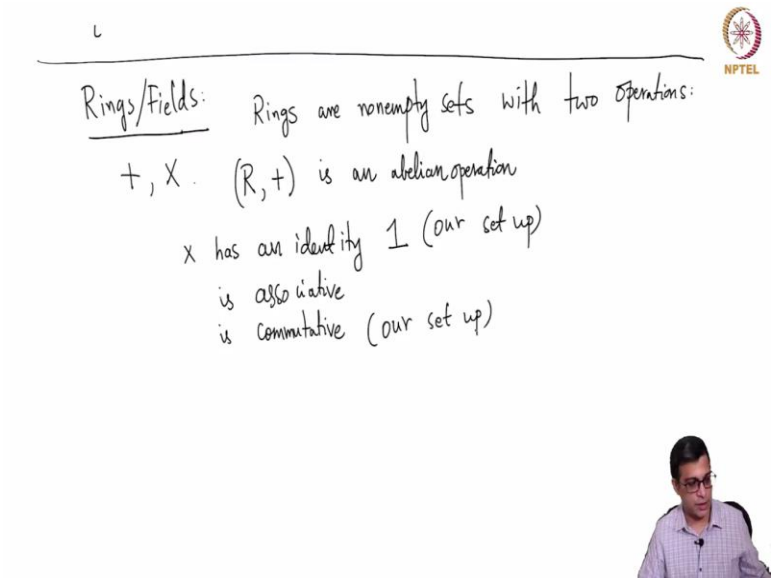
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Review of Ring Theory – Part 1

(Refer Slide Time: 00:14)



So far, we have outlined what we do in this course, what we plan to do in this course on Galois theory. And I told you that in the initial videos, I will recall some of the basic concepts of Group theory, Ring theory, Field theory that we will need. So in the last video, I recall facts about group theory that we required.

(Refer Slide Time: 00:35)

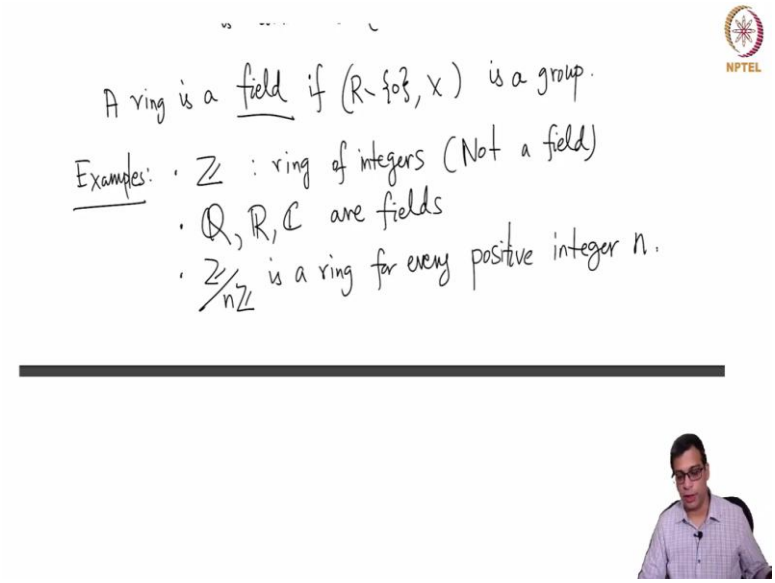


So today, I am going to start recalling what we need to know about Rings and Fields. And as I commented, last time, these are obviously not going to be exhaustive revisions, I am only going to quickly tell you the key and important results and properties of these rings and fields that we require constantly that we require and use in this course on Galois theory. So, if you recall group I recall for you last name is a non empty set with 1 operation rings are non empty sets very briefly non empty sets with 2 operations.

So, we usually denote them by plus and into addition we call them and multiplication and if R is the set which has 2 operations, it is an Abelian group under the addition operation one of them. So, that is one of the requirements and so, in other words, it has an additive identity which we call 0 and you have multiplication is not necessarily a group operation. So, and into has some of the properties the multiplication has some of the properties has a multiplicative identity has an identity, has an identity denoted by 1, 0 is always the additive identity, it is associative and it is commutative.

So, these are the assumptions we will make, this is our setup. So that there is a multiplicative identity is our assumption similarly, that multiplication is commutative is an assumption that we make, you can also consider rings where these are not true. And that is a separate theory. But associativity is always required. What we do not require is inverses.

(Refer Slide Time: 02:56)

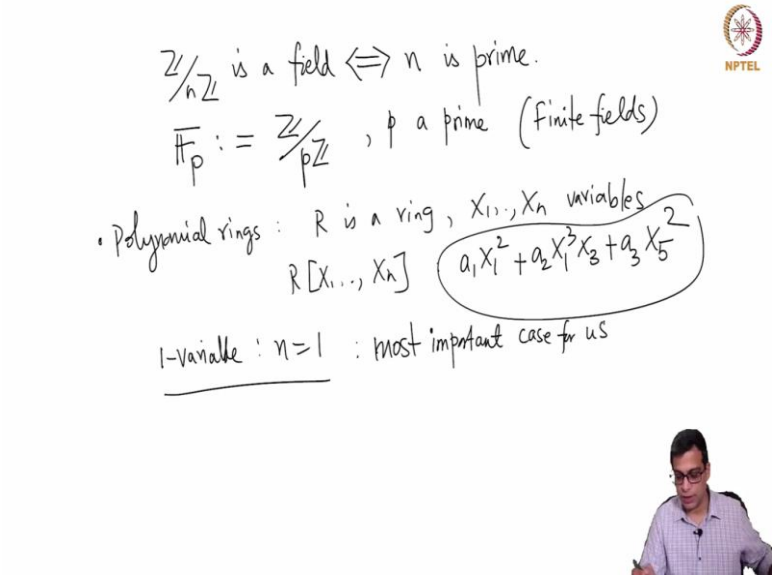


So the typical examples are the most important examples for us, so before I write the examples, also I will mention what is Field? A Ring is a field fields are special types of rings, if R minus 0 is a group under multiplication, so suddenly you cannot put 0 and expect that there is a group operation because 0 cannot be multiplied with anything to get the identity element one. So, 0 cannot have an inverse. But if every nonzero element has an inverse we talk of, we will say that it is a field.

So the main examples, so this is not a course on Ring theory and Field theory, where you study these in general, but in Galois theory, the main examples that we will mostly be looking at are Z of course, is the Ring of integers. This is the first thing that we study. And this is not a field because multiplication does not have inverses, 2 does not have an inverse. Whereas Q, R, C are fields. So they are rings, and they are also fields.

Also, we can consider Z mod pZ, or in general Z mod nZ. So these are classes of rings that I am writing, Z mod nZ is a ring for every positive integer. This is an important thing for us, integers modulo n, so you can go modulo on ideal, and that gives you a quotient ring. So again, I am not discussing those in detail.

(Refer Slide Time: 04:43)

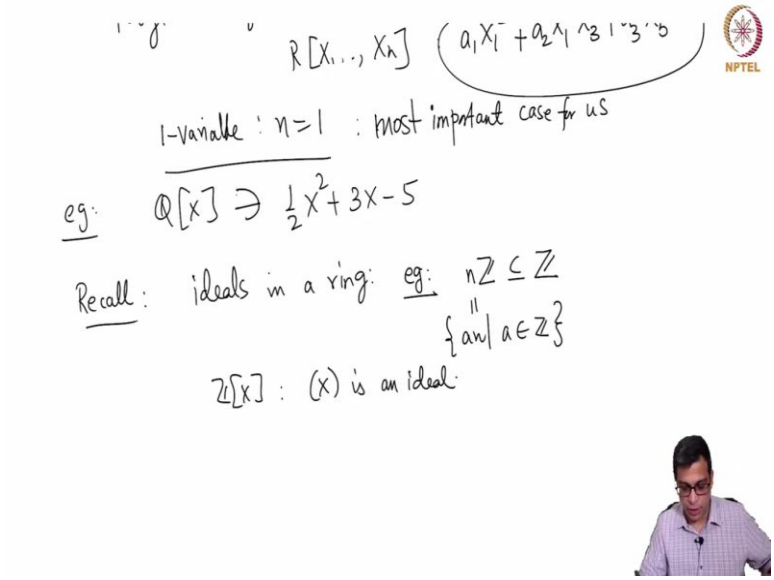


And we know that that mod nZ is in fact a field if and only if n is prime. So that is another fact about. In fact, here I can also admit 0 so, I will say non negative integer when you take n equal to 0 you get the integers itself Z itself. So, this is another important class of fields for us. So, we usually denote Fp to be Z mod pZ, p a prime. So, these are special kinds of fields, these are called finite fields, because they have only finitely many elements.

And another important class of rings for us is the Polynomial Rings. So, if R is a ring and x1 through xn are variable, so, these are indeterminate, they have no meaning they are just symbols. You can consider polynomial ring in n variables over the ring R. So typical elements are things like this. So maybe a1, x1 square plus a2 x1 cubed x3, a4, a3 I mean I am just randomly writing something. So things like this.

So often we will be interested in polynomial rings in one variable, one variable rings are one variable means this means n equal to 1. This is often the most important case for us in this course, but we can also look at other examples 2 variables and so on. So, case for us in this course, the most important example is n equal to 1.

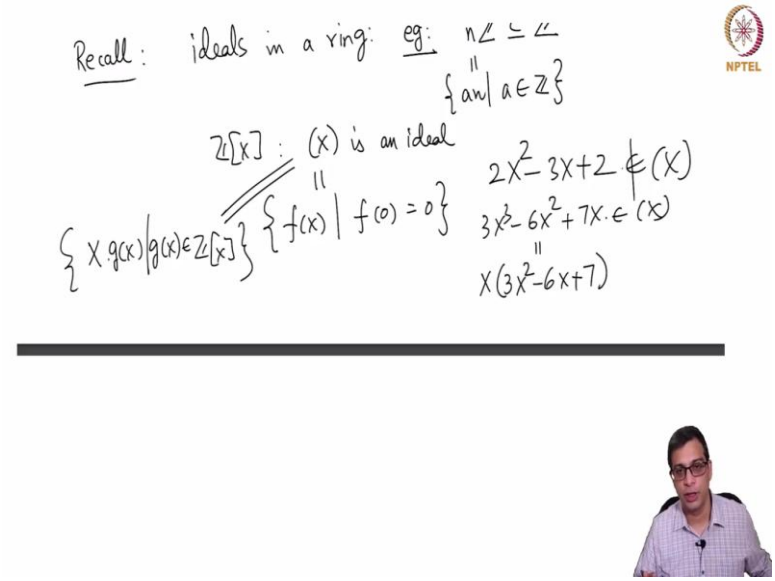
(Refer Slide Time: 06:47)



So, that means we look at for example, polynomial rings in one variable over rational number. So, here it will be things like this, so, this belongs to this. So, if I have only one variable I typically denote that by x. So, these are some of the important examples of rings in this course, and recall also the notion of ideals. I am not define this, but ideally the ring is a subset of a ring, which is a subgroup under addition, and it is closed under multiplication by any ring element.

So, again the typical examples I will give, so, you will recall the definitions in case you forgot you will recall them after this class, but typical examples are nZ in Z, so, this is all integers of the form an, a in Z. So, these are multiples of n. In Zx, x is an ideal.

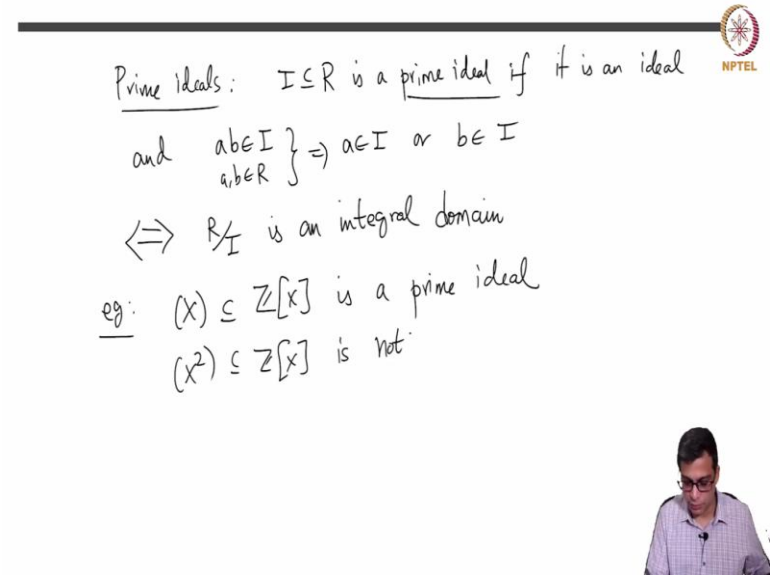
(Refer Slide Time: 08:00)



So, x is an ideal it is defined to be all polynomials where the constant term is 0. So, it must be so remember the definition of is that it is x times some ring element. G is arbitrary. So, which is to say that every const, every polynomial whose constant term is 0 must be a multiple of x obviously, because if you take, let us say 2x square minus 3x plus 2, this is not in x, because you cannot multiply this with x.

Whereas, 3x cube minus 6x square plus 7x is in x because this is simply x times 3x square minus 6x plus 7, again, I am not giving you full definitions or precise definitions, but just giving you a flavor of what ideals are, ideals are very important in ring theory, just like subgroups are important in group theory, ideals are important in ring theory.

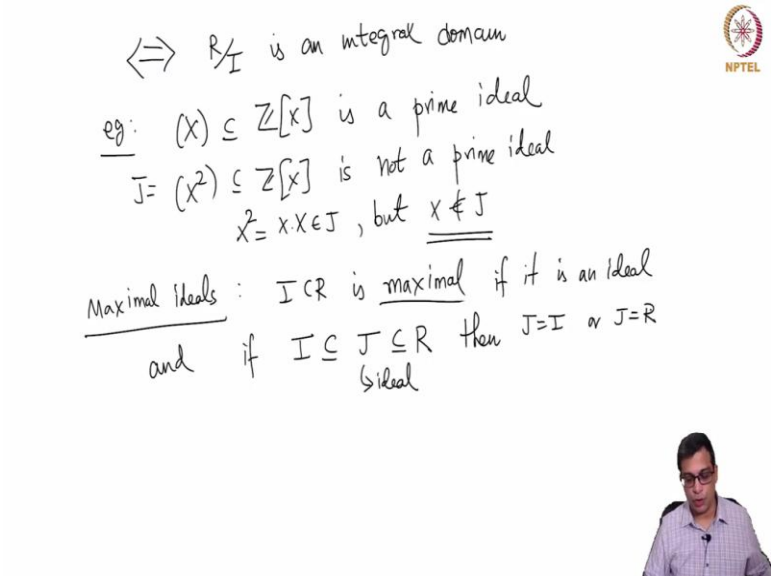
(Refer Slide Time: 09:13)



And we have special classes of ideals called Prime Ideals and Maximal ideals. So, quickly recall what is a prime ideal, so I in R is prime, is a prime ideal or we say it is prime. If of course it is an ideal in addition to being an ideal and it has a property that ab in I implies a and b are R and ab in I implies that a in I or b in I. So equivalently we say that R mod I is an integral domain. These are important notions and terminologies which you should recall before we go further in this course.

Integral domain means no nonzero divisors, that means if you multiply 2 nonzero elements, you get a nonzero element. So, examples the ideal we considered earlier is a prime ideal whereas x square in the same ring is not a prime ideal.

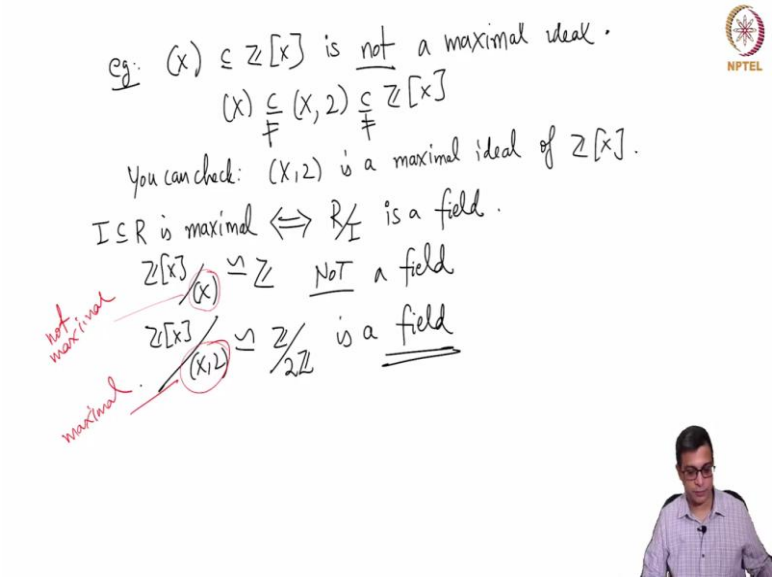
(Refer Slide Time: 10:22)



Because x times x is there in this ideal J. So x times x which is x square is in J, but x is not in J you cannot write x as a multiple of x square because if you multiply by x square the degree is at least 2. So, x itself cannot be in the ideal. So, it is not a prime ideal. The other important class of ideals is called Maximal Ideals and as the name suggests, these are ideals which are maximal.

So, I in R is maximal of course, if it is an ideal I will write it to emphasize that and if I is contained in ideal J which is contained in R, this is an ideal. Then either J is equal to I or J equal to R. So, you cannot have an ideal proper idea that is strictly bigger than I. So, those are maximal ideals so in the class of proper ideals they are maximum elements. So, this is a maximal ideal.

(Refer Slide Time: 11:26)

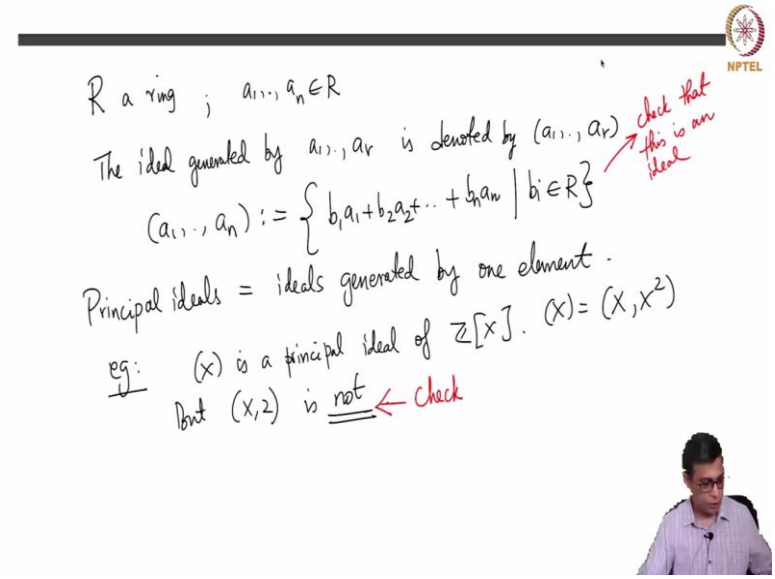


Example, the prime ideal earlier that we considered you can think about it and conclude that it is in fact not a maximal ideal. Why is that? This is clear, because if you take ideal generated by x comma 2 it is not equal here and it is not equal here. So, this is contained in a bigger ideal, which is a proper ideal also.

So, this is not a maximal idea. So, in fact, you can check that x2; x comma 2 is a maximal ideal of Z. You cannot construct a proper ideal which strictly contains the ideal x comma 2. So, also this is a useful criterion. An ideal is maximal if and only if, R mod I is a field. So, you can see that Zx modulo x is isomorphic to Z not a field which confirms the fact that x is not a maximal ideal.

On the other hand, if you go modulo, sorry Zx modulo x comma 2 this is in fact isomorphic Z mod 2Z because you kill x so, then you remain with Z and then you kill 2 in Z so that will give you Z mod 2Z so, this is a field. So, that means, this is not maximal and this is maximal. So, that tells me that you have these are important notions Prime ideals and Maximal ideals. So, one thing that I should probably just clarify or maybe recall for future use.

(Refer Slide Time: 13:51)

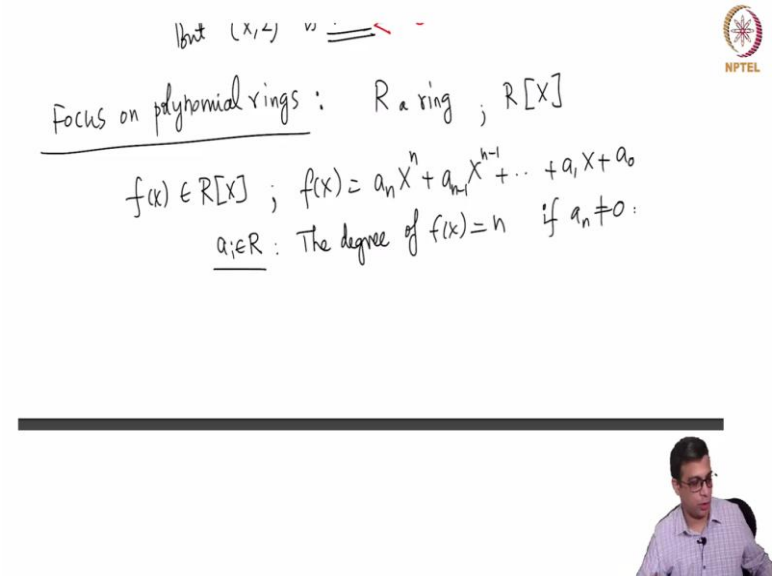


If you have a Ring R and you have elements a1 through an in R the ideal generated by them is denoted by a1 through ar brackets and this is simply you take all ring elements bi's and take this bi are arbitrary ring elements. So, you can check that this is an ideal which is a very easy check. So, this is the ideal generated by a single element by R elements. Now, if you take one element you get what is called. So, this is Rn principle ideals or ideals generated by one element.

So, again example, x is a principal ideal of Zx, but x comma 2 is not, this requires some thinking. Because the point is, even though I have defined this to be generated by 2 elements, it is conceivable that there is some other element, which generates this. For example, x can also be written as x comma x square. I mean, I can always give 2 but I do not need the second one.

So here, you have to argue this, you have to argue that there is no single element, which generates this, so this is a good exercise to recall and refresh your ideas about Rings and ideals. So these are the notions of principal ideals, prime ideals, and maximal ideals. Just to continue this. So a few more theory, things about ring theory.

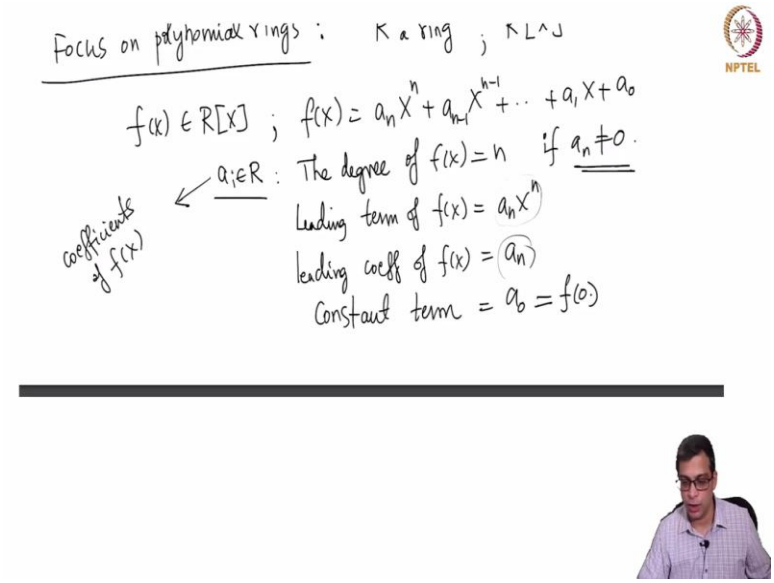
(Refer Slide Time: 16:10)



So, now let us focus on Polynomial Rings. Because this is going to be at the heart of this course. So I am going to use several things about polynomial rings constantly in this course. So let us recall some important results about Polynomial Rings. So let us stick to a general case as much as possible.

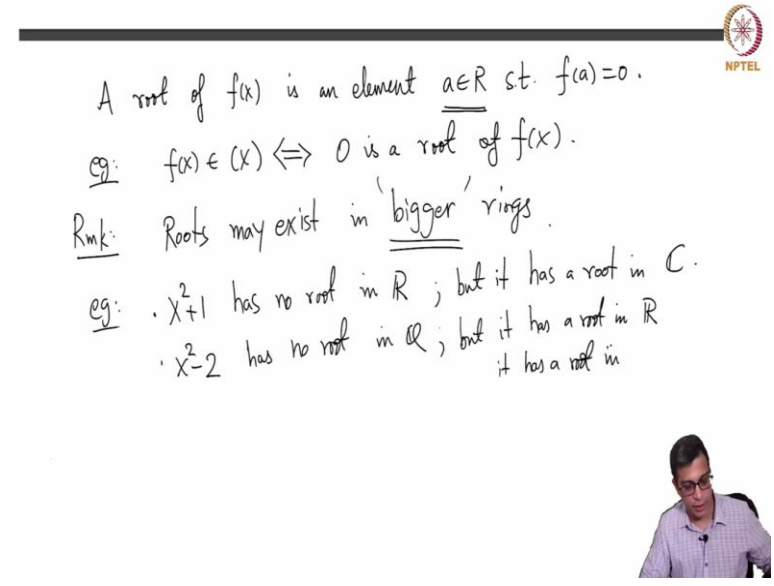
R is a ring and let us consider in fact polynomial rings in one variable, so our Rx so, if fx is in Rx we the general description of fx is like this an Xn, an minus 1 Xn minus 1 a1X plus a0 and recall that it is a ring, it is a polynomial over R, which is to say that ai are all in R. So, the degree of fx is called n if an is nonzero, you can always add 0s in the beginning which we do not want to do.

(Refer Slide Time: 17:17)



So, if an is nonzero, it is called the degree is called n in the leading term of fx is a an Xn. So the highest degree term and the leading coefficient of f is an. So, the leading term is the entire first term and the leading coefficient is just the coefficients of the leading term. So ai's are called the coefficients and the constant term is a0. So that means this is the degree 0 term. So that is constant. And that as I noticed earlier, it is actually just f0. When you plug in 0, all the x terms will go away, and only the constant term remains.

(Refer Slide Time: 18:14)

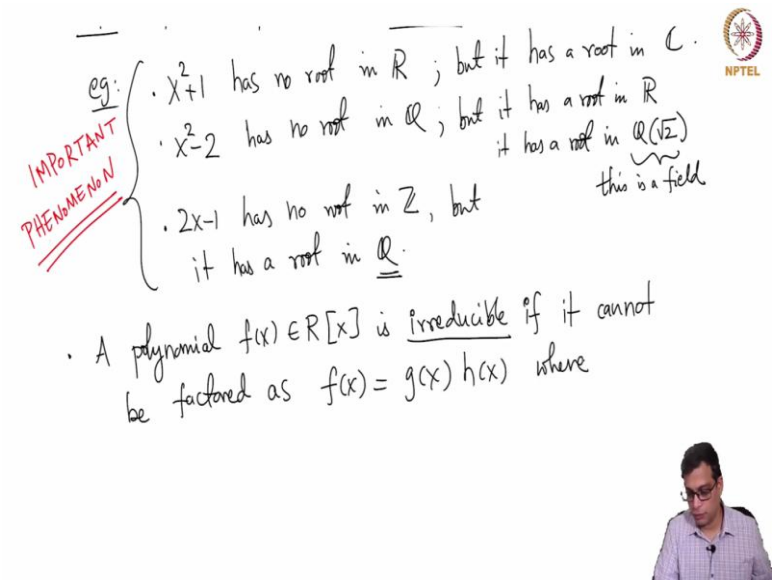


So now, what is the root of such a polynomial? A root of fx is an element a in R such that fa is 0. So the routes may not live in the ring R itself, maybe there is a bigger ring which contains the roots. So this root should be thought of as some element in an extension ring of R. But for now, let us say root is an element a in R such that fa is 0.

For example, one thing you can say is that fx is the ideal generated by x if and only if 0 is the root of f. So, 0 is the root of f if and only if you have the ideal is in the element polynomial fx is in the ideal generated by x itself. So now, remark is that roots may exist in bigger rings.

So, this is somewhat vague, what do you mean by bigger ring is an extension ring. So again example so x square plus 1 has no root in R it is a polynomial over R, but it has no root in R, but it has a root in C. For example, the imaginary number i is a root of this. Similarly, x square minus 2 has no root in the rational numbers, but it has a root in R. But in fact it also has a root in much smaller ring than R.

(Refer Slide Time: 20:11)

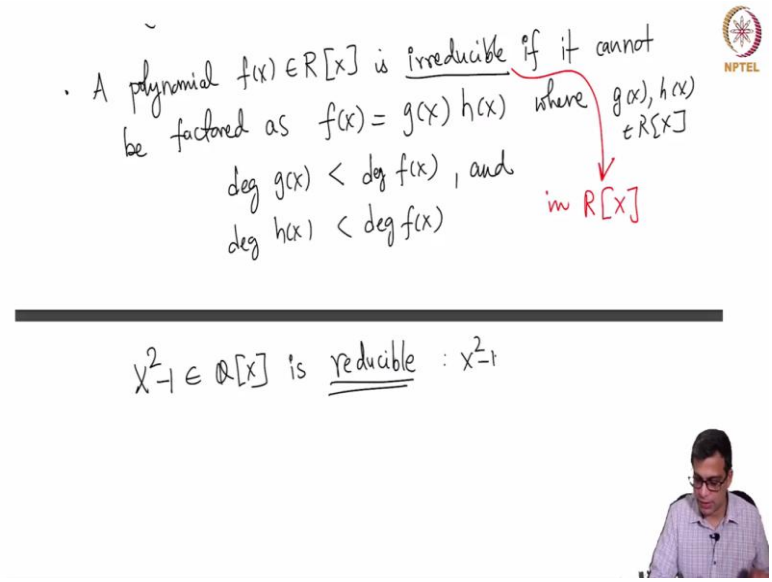


For example, you can take Q adjoined root 2. So in my review field theory, I will describe this later in detail but suffice for now to say that this is a field. So it does not have a root in Q because square root 2 is not rational, however, it is taking a slightly bigger root bigger field you get a root. On the other hand, 2x minus 1 has no root in Z but it has a root in Q, 1 by 2 is its root, but it is not a real, it is not an integer. So, it has no root in Z, but it has a root in, it has root in rational numbers.

So, this is sort of important phenomenon for us. The course will analyze the situation where you have a given polynomial over a given ring the ring itself will not contain roots, but you can construct roots in a bigger ring. So important phenomenon I will write it like this for now. So, this is an important phenomenon for us in this course. So, now continuing this a polynomial is irreducible polynomial fx.

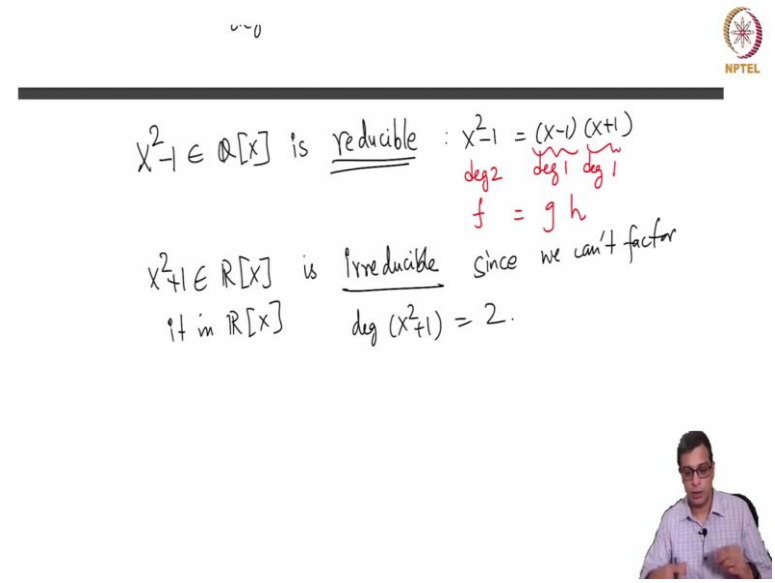
So, I told you that Rx the polynomial ring is a ring so, you know how to multiply 2 polynomials. So, addition is also easy, you just add like terms degree wise, but multiplication is a bit more tricky, but you all know what multiplication of polynomials in Rx is. So, we call this irreducible. A polynomial is irreducible if it cannot be factored as fx equals gx times hx where, where.

(Refer Slide Time: 22:20)



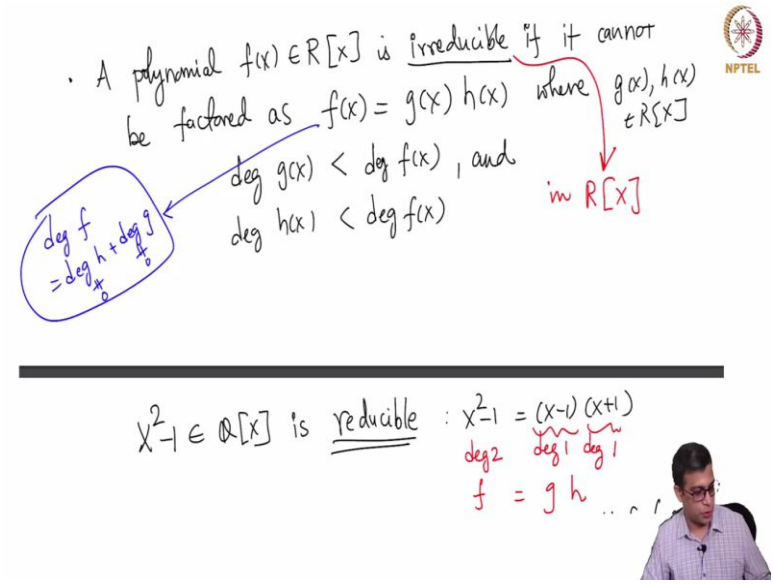
So, I will give you the easy definition here where degree gx and degree hx is less than. So, of course, you can always write the polynomial as 1 times itself so, that is not allowed because the degree does not drop. So, you cannot factor it into product of 2 polynomials which both have smaller degrees. For example, X square and I want you to emphasize here irreducible here I should write in Rx because irreducibility is a property of the ring, which you are working with. So, irreducible in Rx if it cannot be factored as this where g and h are in of course Rx.

(Refer Slide Time: 23:37)



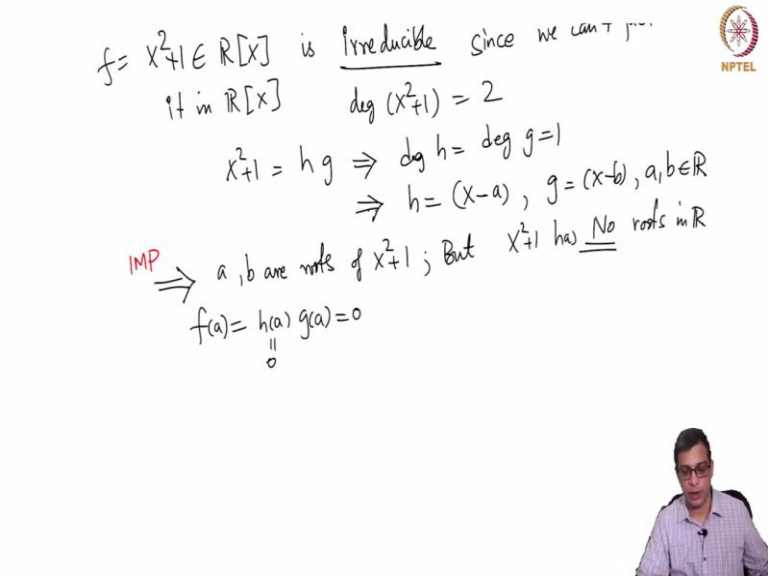
So, if you take x square minus 1 in Qx is reducible. So, if something is not irreducible, we call it reducible, since, you can factor this as x minus 1, x plus 1. So, this you can see is degree 2, this is degree 1 and this is degree 1. So, this is f, you have written it as g times h, where g and h have both degrees 1 which is less than degree of f which is 2. On the other hand x square plus 1 in Rx is irreducible. Since we cannot factor so, this you have to convince yourself because if you could factor degree of x square plus 1 is 2, so, if you can factor it in a valid way, it has to be degree 1 and degree 1.

(Refer Slide Time: 24:35)



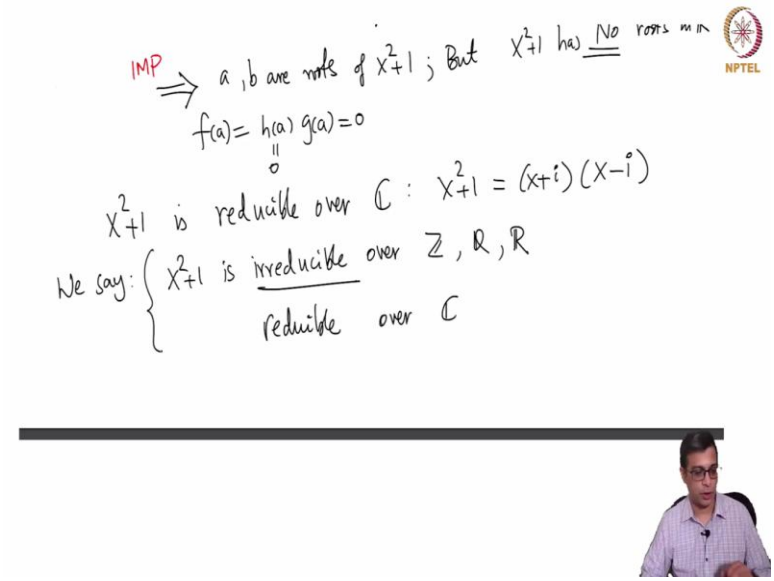
Because also remember, when you write like this degree of f must be degree of h plus degree of g. And both are nonzero. Both are Yeah, so, that is another way of saying this. Because if one of them is 0, the other is equal to degree of f. I am asking both of them to be strictly less than degree of f. That means both are nonzero. So these are all non negative numbers.

(Refer Slide Time: 25:05)



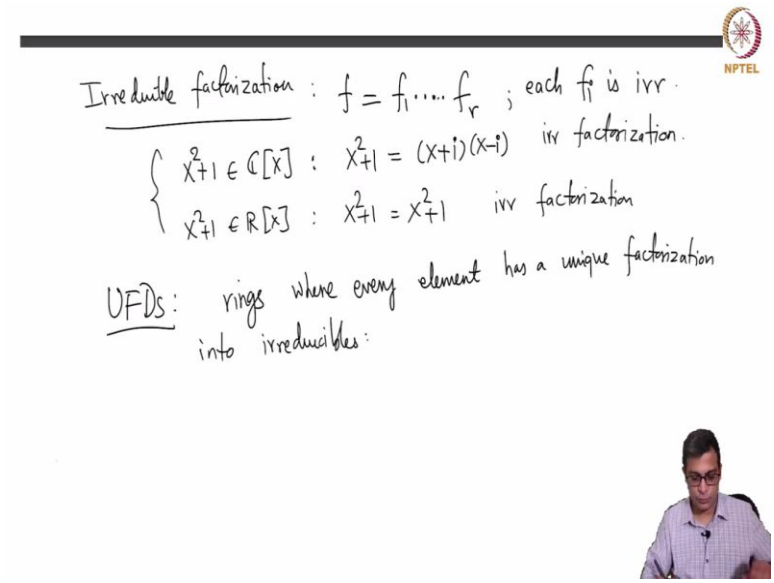
So, if you factor this as product of 2 polynomials, h and g, that means degree h is 1. And degree g is also 1 because it has to be strictly less than 2. But that means h must be of the form because these are monic, you can always write like this where ab are real numbers. So, you can write it like this, but then this is the important observation. So, this is important. a and b are roots of x square plus 1, because if you do call this f, so f of a is h of a times g of a that is 0 because h of a 0. But, of course, you know, x square plus 1 has no roots. So, I have essentially proved that it is irreducible because it does not have roots.

(Refer Slide Time: 26:14)



On the other hand x square plus 1 is reducible over R, over C, sorry. Because x square plus 1 can factor as x plus i times x minus i. So, you do have factorization in Cx and not over Rx. So, we say the terminology is that we say that x square plus 1 is irreducible over Z, Q, R, because the same logic that I gave here, that it does not have roots in R obviously implies that it does not have roots in, it does not have roots in Q as well as in R in Z. So, it is irreducible over that, but it is reducible over C. So, this is the terminology that we want to follow. So now we can talk about irreducible factorization of polynomials.

(Refer Slide Time: 27:15)

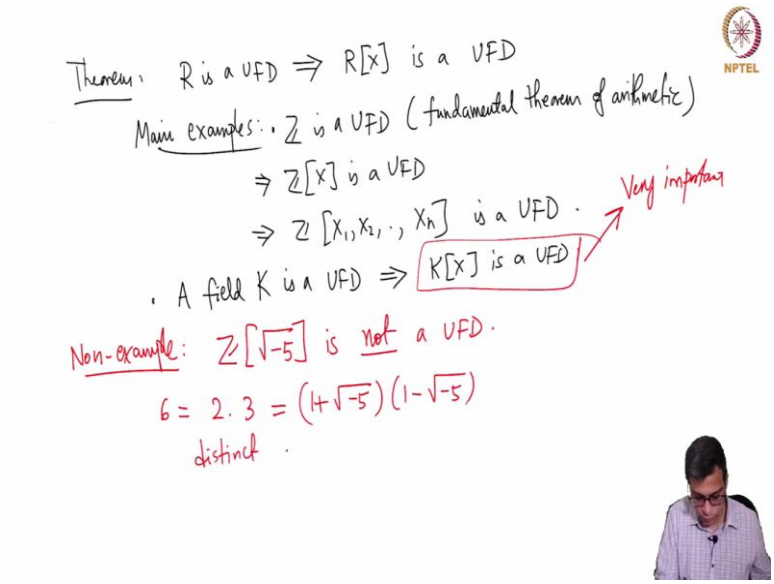


Again, I do not want to get into technicalities here quickly, I just want to essentially give you an idea of what happens it is simply an irreducible factorization of a given polynomial is simply a product as irreducible polynomials so each fi is irreducible. So, for example, x square plus 1 in Cx has irreducible factorization x square plus 1 equals x plus I times x minus i. So, this is the irreducible factorization.

But in Rx it is already reducible. So, x square plus 1 is x square plus 1, this is the irreducible factorization, here it is the irreducible factorization. So, this is irreducible factorizations and then there are some technicalities involved what is allowed what is not allowed and whether they are unique or not, I do not want to get into all those details.

So, UFDs are irreducible rings where there is a unique so I do not want to again define UFDs in full generality rings, where I will not define it in full technical details, but quickly the definition of UFDs is that rings where every element has a unique factorization into irreducibles.

(Refer Slide Time: 29:32)

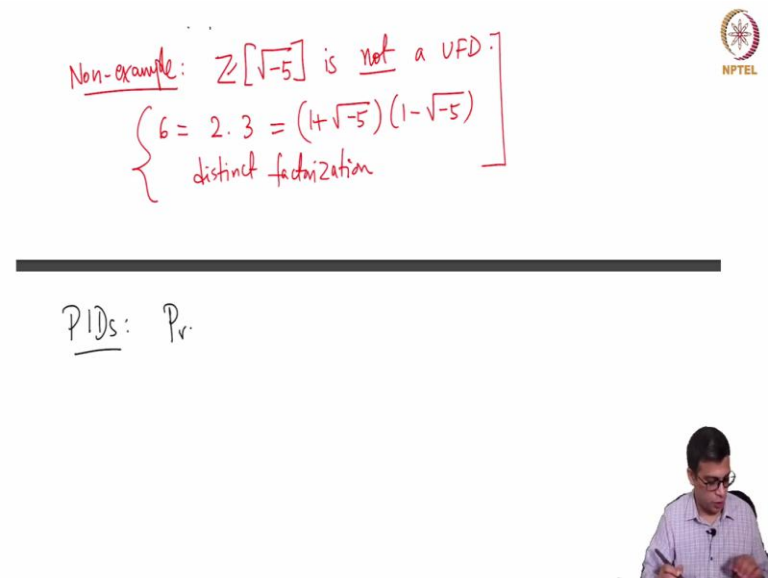


So, the main theorem that we will recall at this point is if R is a UFD then Rx is a UFD. So, this is covered in many courses on ring theory, the main examples of this are so, Z is a UFD so Z is a UFD is a statement that you learn in school in essentially. So, this is the fundamental theorem of arithmetic. So, every integer can be written as a product of prime numbers in a unique way.

So, Zx is a UFD in fact, because that Zx is a UFD you can take 2 variables, 3 variables, 2 variable polymeric polynomial ring over a 1 variable polynomial ring. So, continuing like this inductively you conclude that this is a UFD. Similarly, if field K is a UFD, so, implies Kx is a UFD. This is in fact the most important statement for us polynomial ring in 1 variable over a field is UFD is a very important fact for us.

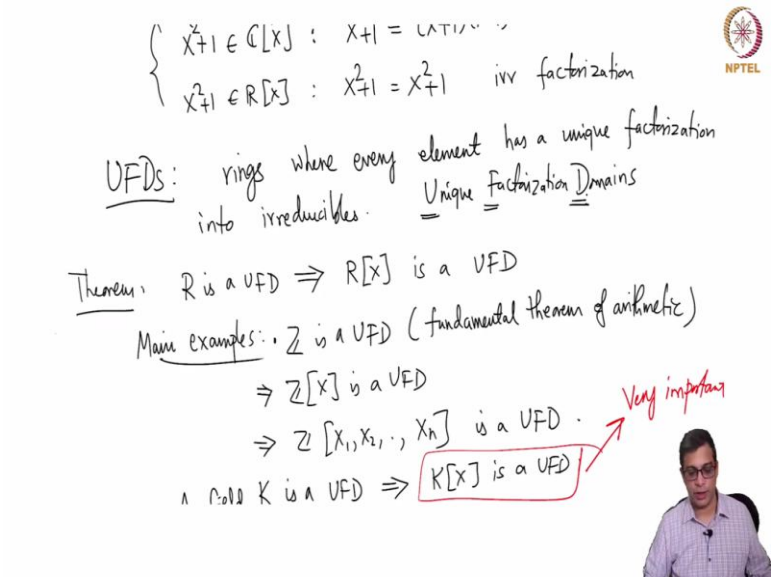
Some other some other examples UFDs or rather non UFDs. So, this is a non example. So, if you take Z adjoined square root minus 5 is not a UFD. This is covered in my Ring theory course for example, or you can look up any book in Ring theory. Here it turns out that 6 the element 6 has 2 factorizations. So, these are distinct factorizations.

(Refer Slide Time: 31:54)



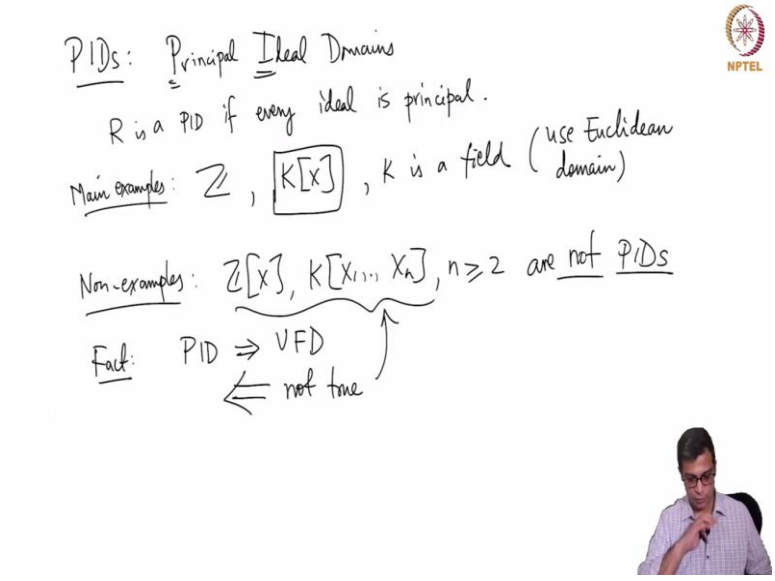
So, again this will rarely come up for us in this course or in fact never it will probably never come up, but I just wanted to give you an example of a ring which is not UFD. An important another important class for us is called PIDs.

(Refer Slide Time: 32:19)



So, this is a short form for, UFD is a short form for Unique Factorization Domains. So, factorization is unique and they are domain so, they are integral domains.

(Refer Slide Time: 32:34)



So, PIDs are Principal Ideal PI Domains. So, these are rings, R is a PID if every ideal is principal. These are very special classes of rings. And the main example for us or main examples, let us say Z and this is again Euclidean division you take an ideal in Z every it must be generated by the least positive integer in that ideal. Similarly, KX, where K is a field. A field is automatically a PID because field has only 2 ideals, the unit Ideals and the 0 ideals.

But the more important example is polynomial rings in 1 variable over a field are PIDs. And the key idea here is use Euclidean division both in the case of integers and polynomial rings over a field in 1 variable, are integral, are PIDs because in the case of integers, you take the least positive number in that ideal, in the case of polynomial rings in 1 variable over a field you take the column with the least degree in that ideal and then you apply division algorithm conclude that, that those elements generate those ideals.

Non examples ZX and KX 1 through Xn where n is greater than equal 2 are not PIDs. These are UFDs they are very nice UFDs, nice rings namely the (())(34:28) but they are not PIDs. So, an easy fact you can check this is again covered in an algebra course is that if something is a PID implies it is a UFD converse not to as these examples show. Zx and KX1 through Xn where n is at least 2 are UFDs but they are not PIDs.

So, let me stop this video. So in this video we recalled Ring theory some important theorems in ring theory, we talked about Prime ideals, Maximal ideals in a ring. We talked about Factoring Polynomials. We talked about what roots of polynomials are, we learned, what are, we recalled rather. What are you UFDs and PIDs. And I told you that UFDs are very common and almost all the rings that we study you are UFDs, whereas PIDs are less common.

But in fact, though, the main interesting Rings that we study in this course are PIDs. So in the next video, I am going to recall another important notion in ring theory called Irreducibility criteria. So these are important things for us because later on in the Galois theory course, we are going to need to determine whether a given polynomial is irreducible or not. So in this video, I will stop now, but I will start the next video by recalling some of the important techniques for determining if a polynomial is irreducible or not. Thank you.